

GAO

Report to the Chairman, Committee on
Science, Space, and Technology, House
of Representatives

February 1991

SPACE SHUTTLE

NASA Should Implement Independent Oversight of Software Development







United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

B-242053

February 22, 1991

The Honorable George E. Brown
Chairman, Committee on Science, Space,
and Technology
House of Representatives

Dear Mr. Chairman:

This report responds to the former Chairman's request of February 13, 1990. It discusses NASA's progress in improving independent oversight of shuttle flight software development.

As arranged with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. We will then give copies to appropriate congressional committees, the Administrator of NASA, and other interested parties upon request.

This work was performed under the direction of Samuel W. Bowlin, Director for Defense and Security Information Systems, who can be reached at (202) 275-4649. Other major contributors are listed in appendix II.

Sincerely yours,

A handwritten signature in cursive script that reads "Ralph V. Carlone".

Ralph V. Carlone
Assistant Comptroller General

Executive Summary

Purpose

The space shuttle is controlled largely by five on-board computer systems. Bugs in these systems' software can cause mission failure, loss of vehicle, even loss of life. Because each shuttle flight is unique, each requires changes to thousands of lines of computer code. Since fiscal year 1981, the National Aeronautics and Space Administration (NASA) has spent more than \$324 million developing, testing, and implementing shuttle software to support commercial projects, scientific research, and defense missions. Software has never been reported as a major problem in shuttle operations.

In early 1988 the National Research Council (NRC) and the House Committee on Science, Space, and Technology expressed concerns about the lack of independent oversight of shuttle software development. Although NASA believed its procedures to be sound, it expanded an existing contract with Intermetrics, Inc. (a contractor not involved in shuttle software), to independently assess shuttle software development. It also established a steering group of knowledgeable NASA and contractor representatives (from both within and outside the shuttle program) to recommend changes where appropriate. In February 1990, the House Committee requested that GAO determine NASA's progress in improving independent oversight of shuttle software development.

Background

NASA successfully flew 24 shuttle missions from 1981 until the Challenger accident in January 1986. Following that accident, NASA delayed shuttle launches to study its procedures for detecting, assessing, and handling hazards and potential shuttle system failures. At NASA's request, NRC reviewed shuttle program procedures. In January 1988 NRC reported the software development activities to be well run, with good quality control. However, NRC questioned the independence of NASA's flight software verification and validation (v&v)¹ process because NASA uses the same contractors to develop, verify, and validate critical software. NRC recommended that the shuttle program vest responsibility for software v&v in independent entities outside the contractor and program organizations that develop the software.

In March 1988 the House Committee on Science, Space, and Technology, echoing NRC's concerns, told NASA it believed the lack of independent v&v of critical software was a serious deficiency. On the basis of its own

¹V&V involves the analysis and testing of software throughout its life cycle to ensure that it meets specified requirements and functions. Requirements for describing, performing, and monitoring these activities are delineated by industry software development standards and federal guidelines for software management.

evaluation, the Committee recommended that NASA establish independent v&v to evaluate the development and modification of shuttle software. The NRC and Committee concerns are based on a generally accepted principle that if an undetected software error has the potential to cause death or personal injury, catastrophic equipment loss or damage, or mission failure, independent v&v is needed. NRC's position that independent v&v be located outside the contractor and program organization is consistent with current NASA-wide software assurance guidance.

Results in Brief

NASA has yet to commit to independent v&v for shuttle software development, and it has moved slowly in establishing v&v policies and documenting existing v&v practices. In May 1988 it expanded Intermetrics' contract to assess current v&v practices, as well as serve as an independent agent to verify and validate shuttle software. In June 1988 it formed the steering group. However, in 1991 the shuttle program plans to discontinue funding Intermetrics in its role as an independent v&v agent for shuttle software because shuttle program officials concluded that Intermetrics' recommendations from its v&v work have not contributed significantly to the overall quality of shuttle software development or quality assurance. Program officials also stated that NASA's record in producing reliable software is sound, and that the funds spent on independent v&v could be better spent elsewhere in the program. Without independent v&v, NASA's software development structure will be about the same as what was in place at the time NRC and the Committee expressed their concerns in 1988.

NASA's shuttle software steering group met only once, in June 1988. Although the group was dissolved before completing its mission of recommending specific improvements, it identified the need for a policy setting forth v&v expectations and documentation of v&v activities. This position is consistent with NASA's own guidance, other federal agencies' requirements, and NRC recommendations. The group also believed an independent v&v oversight office should be formed to closely monitor all software v&v activities. Shuttle program officials stated they are developing a v&v policy and documenting practices. However, they added that sufficient oversight is already being achieved with the program, and establishment of an independent oversight office is not needed.

Principal Findings

Virtually No Progress Made in Improving V&V

Software v&v is critical to the success of the shuttle program. Without it, software performance, integrity, reliability, safety, and quality cannot be reasonably assured. For programs such as the shuttle, where software problems could cause mission failure or even loss of life, the need for independent v&v is generally recognized. Almost 3 years have passed since concerns were raised about shuttle software and NASA has yet to fully address them. To its credit, in 1988 the program did expand an existing contract with Intermetrics at a cost of \$4 million annually to independently verify and validate shuttle software. However, the program has only implemented 6 of 219 recommendations made. The remaining 213 were either dismissed, scheduled for implementation in future versions of software, or are pending review.

Also to NASA's credit, it now appears to be addressing issues raised by the shuttle software steering group in 1988 concerning documentation of existing v&v practices and establishment of a shuttle software v&v policy. However, as of December 1990, NASA has yet to complete this effort.

Shuttle Program Office Plans for Addressing V&V Independence Are a Step Backwards

NASA plans to phase out Intermetrics' independent v&v by the end of fiscal year 1991. Program officials stated that Intermetrics' recommendations have added little value, and that the problems it found were either insignificant or would have been caught by NASA's own quality assurance processes. According to these officials, NASA's previous success in producing high quality software, along with its opinion of Intermetrics' recommendations, suggest that the \$4 million a year can be better spent elsewhere.

The program office plans to ignore the software steering group's views on the need to establish an independent v&v oversight office. Program officials contend they do not need a separate office to ensure that all v&v activities are effectively integrated into a coherent and coordinated process, and that all contractor and NASA organizations and facilities perform required v&v activities. However, GAO believes that no single mechanism currently exists to provide these assurances.

Program officials contend that current shuttle software v&v practices provide an adequate level of independence between the software developers and those that ensure that it works properly. GAO disagrees. Not only is this position contrary to NRC and House Committee recommendations, it is not consistent with NASA-wide software assurance guidance, which encourages independent v&v to be performed by someone with no stake in the software, and who is neither the developer nor the acquirer.

While GAO recognizes that NASA might have to rely on its network of contractors and facilities to conduct v&v, the criticality of software to a multibillion-dollar, manned space program suggests the need for effective independent v&v outside the software development contractor and the program office.

Recommendations

GAO recommends that the Administrator, NASA, require independent v&v for shuttle software, bearing in mind the views of NRC, the House Committee, the software steering group, and NASA-wide guidance, and ensure that the independent v&v organization is outside the control of the shuttle program office. In addition, GAO recommends that the Administrator bring to closure the issues raised by the software steering group concerning policy and documentation of v&v activities. In this regard he should require the steering group to provide formal recommendations to the shuttle program office. He should then require the program office to provide time frames for addressing them.

Agency Comments

In commenting on a draft of this report, NASA concurred with GAO's assessment of the critical issues associated with the development of shuttle software. NASA identified several positive actions it planned in response to GAO's recommendations on bringing the software steering group's issues to closure. NASA also plans to ask NRC to evaluate the adequacy of the shuttle software v&v process. GAO questions the need for another study—this area has been analyzed several times by different organizations, each reaching similar conclusions that while the shuttle software development activities are good, more should be done. However, given the relatively short time frame established for the study, GAO is not opposed to NASA's obtaining another viewpoint. GAO's position, however, remains unchanged. An appropriate level of independent v&v should be required. In addition, to be truly independent, the v&v office should be located outside the control of the shuttle program office. NASA's comments are included as appendix I.

Contents

Executive Summary		2
Chapter 1		8
Introduction		8
	The Shuttle Is Largely Computer-Controlled	8
	Maintenance of Software Is Costly and Extensive	9
	Verification and Validation Helps Ensure That Software Changes Comply With Requirements	10
	Objectives, Scope, and Methodology	12
Chapter 2		14
NASA Should	Independence of Software Verification and Validation: Is It Adequate?	14
Implement	Several Actions Initiated to Address Concerns	15
Independent Software	Few of Intermetrics' Recommendations Implemented	16
Verification and	NASA's Actions on Steering Group Concerns	17
Validation	Shuttle V&V Approach Seen as Best Available	20
Chapter 3		22
Conclusions and	Recommendations	23
Recommendations	Agency Comments	23
Appendixes		
	Appendix I: Comments From the National Aeronautics and Space Administration	26
	Appendix II: Major Contributors to This Report	29

Abbreviations

ANSI	American National Standards Institute
GAO	General Accounting Office
IBM	International Business Machines, Inc.
IEEE	Institute of Electrical and Electronics Engineers
IMTEC	Information Management and Technology Division
NASA	National Aeronautics and Space Administration
NRC	National Research Council
V&V	verification and validation

Introduction

The National Aeronautics and Space Administration (NASA) established the space shuttle program to provide economical access to space for commercial, scientific research, and Department of Defense projects. NASA's reusable shuttles, each designed to fly 100 missions, are capable of ferrying passengers, cargo, and payloads into orbit between 115 and 250 miles above the earth. NASA has three operational shuttles—Columbia, Discovery, and Atlantis—and plans to add a fourth, Endeavour, by February 1992. It has deployed commercial and military communications satellites and large government projects using the shuttles, such as the Galileo Space Probe and the Hubble Space Telescope; it likewise plans to deploy the Space Station Freedom using the shuttle. It has spent about \$55 billion¹ on the program since the early 1970s.

NASA successfully launched and safely returned shuttles to earth 24 times between April 1981 and January 1986, when the attempted launch of Challenger ended tragically in the loss of the flight crew and the vehicle. For more than 2 years following the accident, NASA delayed shuttle launches while studying its procedures for detecting, assessing, and dealing with hazards and potential shuttle system failures. During that time, NASA contracted with outside organizations to review its procedures and processes and recommend improvements in shuttle operations. The shuttle program resumed flights in September 1988 after making safety-related hardware and software changes to the shuttle systems. NASA flew 12 successful missions between September 1988 and December 1990.

The Shuttle Is Largely Computer-Controlled

The success of every shuttle mission depends on many factors, including the performance of on-board computer systems that are used more extensively on the shuttle than on any previous spacecraft. NASA designed the shuttle to be almost totally controlled by on-board computer hardware and software systems. It found that direct manual intervention was impractical for controlling the shuttle during ascent, orbit, or reentry due to the required precision of reaction times, systems complexity, and size of the vehicle. For example, sequencing of certain shuttle events must occur within milliseconds of the desired times, as operations 10 to 400 milliseconds early or late could cause loss of crew, loss of vehicle, or mission failure.

Five on-board computer systems control and monitor almost every phase of shuttle operations—vehicle systems testing, ascent, orbit,

¹Estimate provided by NASA's Office of Public Affairs, based on current-year dollars.

reentry, and landing. Four of these computer systems are arranged as a redundant set, with each running the primary software independently and simultaneously during the most critical phases of shuttle flight. The mission commander can deactivate a faulty computer system if an error is detected. The fifth computer system simultaneously runs the backup software in such a way that it could immediately take over flight functions if the primary software failed.

The five on-board computer systems are driven by primary and backup software that must be modified for every flight, thus raising the risk to human, vehicle, and cargo. The primary software system controls (or assists in controlling) most of the shuttle systems. Its functions include the automatic determination of the vehicle's status and operational readiness; managing shuttle sequencing controls for the solid rocket boosters and external fuel tank during launch and ascent; performance monitoring; digital data processing; communications and tracking; payload and system management; guidance, navigation, and control; and electrical power distribution for the orbiter, external tank, and solid rocket boosters. Computerized vehicle control is used for every phase of the mission except for docking, a manual operation that must be performed by the crew. NASA officials and contractors generally believe shuttle software is the most complex set of programs ever developed for aerospace use.

The backup software is intended for use only if needed to complete safe shuttle ascent and reentry, maintain vehicle control in orbit, and perform system management functions during ascent and reentry. This software is synchronized with the primary software so that it can track the primary software and keep up with the flow of commands and data. If the primary software fails, the mission commander needs only to press a button to engage the backup software.

Maintenance of Software Is Costly and Extensive

NASA began developing the primary software systems in 1973 and made over 2,000 requirements changes to the initial version of the software between 1975 and 1981. Since the first mission in 1981, NASA has spent more than \$324 million updating and refining basic shuttle software systems. NASA's current and future shuttle missions require that it continue to refine and use shuttle software to accomplish its goals. NASA has announced plans to schedule another 27 missions from January 1991 through December 1993.

Software changes are generally made to correct deficiencies, enhance the software's capabilities, or tailor it to specific mission requirements. Changes are usually included as part of operational increments, which are scheduled updates of the primary and backup software. Each operational increment of software is designed to support a specific number of planned missions, and requires additions, deletions, or changes to thousands of lines of computer code. For example, operational increment number OI8C, which supported four recent flights, required changes to about 73,400 lines of code of software (about 12 percent).

Verification and Validation Helps Ensure That Software Changes Comply With Requirements

The software development and reconfiguration process must produce high-quality, error-free software that NASA can depend on to perform as expected. Software quality assurance, a planned and systematic set of activities to ensure that software processes and products conform to requirements, standards, and procedures, is a critical component of the shuttle program. Two of the supporting software quality assurance disciplines—verification and validation—involve the analysis and testing of software throughout its life cycle to ensure that it meets requirements and functions as specified. Its purpose is to ensure the final product's performance, integrity, reliability, safety, and quality.

Software verification is "the process of determining whether or not the products of a given phase of the software development cycle fulfill the requirements established during the previous phase."² It usually involves reviewing, testing, and documenting that systems' requirements, design, software coding, and documentation conform to specified requirements. Verification leads to improvements in overall software quality and reduced operational costs by allowing early detection of errors and performance problems. Validation is "the process of evaluating software at the end of the software development process to ensure compliance with software requirements."³ It ensures that systems perform intended functions correctly and perform no unintended functions.

The difference between verification and validation is unimportant except to the theorist; practitioners use the term v&v to refer to all of the activities aimed at making sure the software will function as

²IEEE Standard Glossary of Software Engineering Terminology, Institute of Electrical and Electronics Engineers (IEEE), Inc., American National Standards Institute (ANSI), ANSI/IEEE Standard 729-1983, August 1983, p. 37.

³IEEE Standard Glossary of Software Engineering Terminology, p. 37.

required. A primary benefit of performing v&v is to increase confidence in the quality of the software.

Guidance on Performing and Documenting V&V Is Well-Established

Requirements for planning, describing, performing, and monitoring v&v activities are delineated by industry software development standards and federal guidelines for software management. For example, for industry the Institute of Electrical and Electronics Engineers (IEEE) has issued a specific standard requiring that a software v&v plan be prepared for critical⁴ and noncritical software.⁵ For federal application, the National Institute of Standards and Technology has issued several publications that provide guidance covering the basic planning for a v&v effort, selection of v&v techniques and technical tools, and a comprehensive outline of important information that should be included in v&v plans.⁶

Several federal agencies, including NASA, have issued specific guidance for planning and conducting v&v activities. For example, the Department of the Air Force has issued guidance describing a multistep procedure for determining if independent software v&v is needed, establishing its scope, identifying its specific tasks, selecting a qualified v&v agent, and determining its costs.⁷ NASA's Office of Safety and Mission Quality has issued a series of documents aimed at improving the documentation of NASA information systems (including a detailed v&v plan),⁸ and software quality assurance.⁹ NASA headquarters allows programs and projects to individually determine if and how this guidance will be used.

⁴IEEE defines software as critical if its failure could have an impact on safety, or could cause large financial or social loss.

⁵IEEE Standard for Software Verification and Validation Plans, IEEE, New York, N.Y., ANSI/IEEE Standard 1012-1986, November 14, 1986.

⁶Guideline for Lifecycle Validation, Verification, and Testing of Computer Software (FIPS PUB 101, June 6, 1983), Guideline for Software Verification and Validation Plans (FIPS PUB 132, November 19, 1987), Planning for Software Validation, Verification, and Testing (Special Pub 500-98); National Institute of Standards and Technology, Department of Commerce, Washington, D.C.

⁷Software Independent Verification and Validation, AFSC/AFLC Pamphlet 800-5, Department of the Air Force, May 20, 1988.

⁸Information System Life-Cycle and Documentation Standards (5 volumes), NASA, Office of Safety and Mission Quality, Release 4.3, February 28, 1989.

⁹Software Assurance Guidebook, NASA, Office of Safety and Mission Quality, SMAP-GB-A201, September 1989.

Objectives, Scope, and Methodology

On February 13, 1990, the House Committee on Science, Space, and Technology requested that we obtain information on NASA's efforts to improve shuttle software oversight activities, including its efforts toward establishing independent oversight of critical shuttle software processes, in response to concerns raised by the Committee. It also asked that we identify NASA's progress and problems in implementing the v&v recommendations made by an independent NASA contractor, Intermetrics, Inc. In meeting our primary objective we sought to identify (1) NASA's procedures for developing, validating, verifying, and reconfiguring shuttle software; (2) recommendations made by the independent contractor hired by NASA to verify and validate shuttle software; (3) problems hindering NASA's progress in implementing the recommendations; and (4) actions taken by NASA to specifically resolve concerns raised by the National Research Council (NRC) and the shuttle program's software steering group formed to recommend changes in the v&v processes.

To identify procedures for verifying, validating, and reconfiguring software, we

- interviewed NASA officials in the Space Shuttle program's Engineering Integration Office Avionics Office, and NASA's Office of the Inspector General, to identify policies, procedures, and requirements for conducting quality assurance of shuttle software;
- obtained and reviewed documents that describe major entities' roles and responsibilities;
- met with representatives of Rockwell Space Operations Company, International Business Machines, Inc. (IBM), Rockwell International, and Intermetrics, Inc., to discuss their responsibilities, processes, and internal guidelines for developing, verifying, validating, and certifying software; and
- obtained information on the role and responsibility of NASA's Office of Safety and Mission Quality for critical software quality assurance for the Space Shuttle and Space Station programs.

To identify the independent contractor's recommendations, we

- interviewed officials in the shuttle program's Avionics Office and officials of Intermetrics at Houston, Texas' Lyndon B. Johnson Space Center and in Bellevue, Washington; and
- analyzed Intermetrics' reports, summarized the findings, and followed up through discussions with appropriate NASA and Intermetrics officials on the most critical recommendations.

To identify NASA's progress in implementing the recommendations, we

- discussed with NASA officials, software development contractors, and officials of Intermetrics factors they believe affected the acceptance and implementation of the recommendations; and
- obtained comments from Space Shuttle officials, contractors, and Office of Safety and Mission Quality officials on the contractor's overall contributions to verifying and validating shuttle systems software.

To identify actions taken specifically by NASA to resolve NRC and the software steering group's concerns, we

- reviewed NRC's January 1988 report to the NASA Administrator and minutes of the steering group's June 1988 meeting, to identify their concerns; and
- discussed with Space Shuttle officials the status of planned improvements.

Our audit work was performed in accordance with generally accepted government auditing standards, between February and November 1990 at various locations, including the Johnson Space Center and contractors' sites in Houston; Bellevue, Washington; and Huntington Beach and Downey, California.

NASA Should Implement Independent Software Verification and Validation

The shuttle program uses multiple contractors and NASA organizations and facilities for software testing and v&v, to ensure that critical software will perform as expected. NASA considers this approach a strong feature of the shuttle software quality assurance process, which has produced high-quality, dependable software since the first shuttle flight in 1981. However, several organizations, including NRC, a congressional committee, and an internal NASA steering group, have expressed concerns about aspects of the process NASA uses to verify and validate critical software.

In essence, each group believes that NASA could do more to ensure the maximum integrity of shuttle software development by using an independent organization to verify and validate shuttle software. Their concerns are based on a generally accepted principle that if an undetected software error has the potential to cause death or personal injury, catastrophic equipment loss or damage, or mission failure, independent v&v is needed. Although NASA appeared to be off to a good start when these concerns were raised in 1988, it has yet to implement these groups' recommendations. Shuttle program officials believe their processes are the best available, provide a high level of independence, and that no additional oversight is needed.

Independence of Software Verification and Validation: Is It Adequate?

Following the Challenger accident in January 1986, NASA delayed shuttle launches to study its procedures for detecting, assessing, and handling hazards and potential shuttle system failures. At NASA's request, NRC reviewed a number of aspects of the shuttle program and issued a report to NASA in January 1988.¹ The report noted that the existing software v&v process was well run, had good quality controls, and should be retained. However, the report questioned the independence of the process.

The shuttle's primary software is developed under contract by IBM. Another IBM group, that does not report to the IBM software development manager but that serves the shuttle program office under the same contract, carries out independent v&v of the software produced by the development group. After delivery to NASA, the software is thoroughly tested at Johnson's shuttle avionics integration laboratory. NASA considers this multifacility, multi-organizational participation in software testing and v&v to be a strong feature of its process.

¹Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management, Aeronautics and Space Engineering Board, National Research Council, January 1988.

The NRC report noted, however, very close collaboration at Johnson among NASA personnel and support contractors involved in software development, with little clear differentiation of roles and responsibilities. Although the report noted that this atmosphere produced teamwork and cooperation, it did not, according to NRC, promote the maintenance of adequate checks and balances required for truly independent v&v. The NRC report also expressed the belief that Johnson's shuttle avionics integration laboratory was good for software end-to-end testing, but was not adequate to fulfill the purposes of independent v&v.

The NRC report stated that this lack of independence would lead to serious questioning by outsiders if significant software problems ever developed. It recommended that responsibility for the approval of software verification and validation be vested in entities outside the program structure, as well as the centers directly involved in shuttle software development. NRC's position that the independent v&v agent be located outside the contractor and program organization is consistent with current NASA-wide software assurance guidance.²

House Committee Recommends Independent V&V

In a March 1988 letter to NASA, the House Committee on Science, Space, and Technology echoed NRC's concerns, citing similar findings in a study done by its own staff.³ The Committee's work revealed that the lack of independent v&v was a serious deficiency in the shuttle program. Accordingly, the committee wrote to "urge, in the strongest possible terms," that NASA establish an independent v&v activity to evaluate the development and reconfiguration of shuttle software.

Several Actions Initiated to Address Concerns

NASA's administrator responded to the Committee's concerns in May 1988.⁴ Although NASA believed that its procedures were adequate, it agreed to expand an existing contract with an experienced contractor, Intermetrics, Inc., to perform, among other things, independent v&v of shuttle software. NASA also told the Committee it would establish a steering group to examine the software processes and make recommendations for appropriate changes. The group was established in June 1988 and included shuttle program personnel, headquarters officials,

²Software Assurance Guidebook, NASA-SMAP-GB-A201, September 1989.

³Letter to Administrator, NASA, from Chairman, House Committee on Science, Space, and Technology, March 31, 1988.

⁴Letter to Chairman, House Committee on Science, Space, and Technology, from Administrator, NASA, May 9, 1988.

shuttle software contractors, and program consultants. NASA promised that the recommendations of the steering group would be fully addressed by the shuttle program.

Few of Intermetrics' Recommendations Implemented

In expanding⁵ its ongoing contract, NASA officials said they allowed Intermetrics almost total autonomy in developing approaches to accomplishing its work. During the course of its work, Intermetrics issued 219 recommendations to NASA resulting from its v&v work. Six of these were implemented, resulting in changes to shuttle software. Of the remaining 213 recommendations, 51 are awaiting analysis by NASA or software development contractors, or review by the shuttle avionics software control board; 29 were deemed to be minor documentation, or maintenance-related, non-safety issues on which action was deferred. NASA ruled that the other 133 either were not valid or did not require a change to the software.

Program officials told us that some of the deferred recommendations or ones awaiting analysis or review may be implemented in future operational increments. As discussed in chapter 1, only changes that are critical to safety or are needed because of specific mission requirements are made outside of regular operational increments. Intermetrics has not contested NASA's disposition of any of the recommendations. According to the director of Intermetrics' avionics division, its responsibility was to identify and present potential shuttle software problems and recommend solutions to NASA; NASA is then responsible for deciding the appropriate disposition of the recommendations. He further said that Intermetrics generally agrees with NASA's handling of recommendations, and has agreed with NASA in all cases to date. If Intermetrics had disagreed, it could have appealed to NASA headquarters.

Little Value Seen in Intermetrics' V&V Work

Shuttle program officials believe that Intermetrics' v&v work has not added value to the shuttle software development and quality assurance processes. The program officials plan to phase out this work in 1991 because they believe that (1) the program structure for developing, testing, and verifying and validating software is highly effective; (2) the added value to the quality of shuttle software provided by Intermetrics has not been significant; and (3) the money spent on the Intermetrics contract could be better spent on higher priority projects within the Space Shuttle program.

⁵NASA estimated the increased cost for independent V&V was about \$4 million annually.

However, program officials feel that Intermetrics has made contributions to the software development and quality assurance process through other means, largely undocumented and unmeasurable. For example, at NASA's request, Intermetrics participated on ad hoc teams formed to address specific shuttle hardware or software engineering issues. According to NASA, this participation contributed directly to resolving the issues. Intermetrics has also provided NASA with assessments and recommendations related to shuttle hardware and software systems as part of its systems-engineering responsibilities, which are outside the scope of its independent v&v work. NASA has had a contract with Intermetrics since April 1987 to conduct shuttle software and avionics systems engineering, is pleased with this portion of Intermetrics' work, and plans to continue it.

NASA's Actions on Steering Group Concerns

The NASA software steering group^a appointed because of NRC and congressional concerns met once, June 16-17, 1988, to determine if any improvements could be made in the way NASA and its contractors verify and validate shuttle software. Minutes from the meeting were prepared, but were never formally approved by the group chairman. However, the group consensus, which we verified with the chairman and several members, was that definite improvements should be made. Nonetheless, formal recommendations were never prepared or submitted to the shuttle program director or NASA administrator for consideration because the steering group's impetus waned after its chairman transferred out of the shuttle program area.

Steering Group Members Felt More Should Be Done

While discussing the shuttle program's approach to verifying and validating software, minutes from the meeting showed general agreement that the program had all of the basic processes in place to adequately verify and validate shuttle software. However, participants voiced concerns that the program had not adequately documented its v&v procedures, and believed this should be done. Participants also commented that the program should develop a policy on v&v that would, among other things, establish expectations and standardize the nomenclature for describing v&v activities. The improved documentation, combined with the v&v policy, was intended to clearly define NASA's v&v process and help the program measure the level of compliance with shuttle

^aThe 16-member group included key shuttle program officials from Johnson, Marshall Space Flight Center, Kennedy Space Center, and NASA headquarters; software development contractors and consultants; and the space transportation system operations contractor.

software standards, processes, and procedures. It would also bring NASA into closer compliance with IEEE standards and federal guidelines for performing and documenting software v&v.

The minutes from the meeting also showed that although members agreed with NRC's position that the shuttle program had established an effective v&v program, they thought it could benefit from added independence or oversight. Some felt the program should establish an independent oversight office at the Johnson Space Center, likely with contractor support, that reports to NASA's Office of Safety and Mission Quality. Members stated that using an independent contractor would ensure a competitive environment, and placing the function under the safety office would add independence of oversight and be outside the budget control of the shuttle program. They believed that independent reviews of the shuttle program's software development and reconfiguration processes would help ensure that NASA and its contractors were following established standards, processes, and procedures.

Draft Policy Was Circulated but Never Implemented

Although a scheduled second meeting of the steering group was cancelled, in November 1988 the program's avionics office circulated a draft v&v policy statement to steering group members for review and comment. Its purpose, when implemented, would be to establish policy for v&v of shuttle software. To ensure that all program v&v efforts are integrated into a coherent, coordinated process, an independent v&v office would be created, reporting to the program's avionics office.

The independent v&v office would

- define and maintain an overall set of v&v requirements;
- coordinate all test, quality assurance, and v&v activities;
- establish audits, assessments, and other investigative activities to ensure the integrity and independence of v&v processes; and
- manage and direct a contractor that would conduct independent v&v activities on all aspects of the shuttle software development program.

Only 6 of 16 steering group members commented on the draft policy. All agreed that a separate v&v office was needed and offered suggestions for its structure and mission. One commented that to achieve organizational independence, the v&v office should report directly to the deputy program director—not the avionics office.

NASA Is Now Developing a Policy and Documenting Its Processes

We asked shuttle program representatives why the concerns raised at the June 1988 software steering group meeting were never addressed. They told us that although the group got off to a good start, its impetus waned after a shuttle program official, who had also served as the steering group chairman, transferred to NASA's space station program. They said that the group's 1988 concern about the need for a shuttle program v&v policy was still valid, and that one was being developed but had not been implemented as of early December 1990.

Program representatives also told us the steering group's position that the software v&v process be thoroughly documented was also still valid. Although it relies extensively on contractors and various NASA entities in completing the 28-month-long process for developing, approving, and implementing shuttle software, the program has not fully identified and documented these steps. The shuttle program's failure to adequately document software v&v conflicts with a NASA shuttle software policy established in 1979, as well as NASA software documentation standards issued in 1989. For example, the 1979 NASA policy covering software management for flight projects requires all field installations to document—in a software management plan—all mechanisms the project will use to assure the quality of software development, as well as the end products.⁷ Emphasis is placed on the tests that the project will use to verify and validate that the software and hardware systems work together to meet mission specifications. Recent NASA headquarters guidance published in 1989 further describes the importance of performing and documenting software v&v throughout all phases of the software life cycle, from initial concept to operations and maintenance.⁸ NASA's software management plan standards,⁹ as well as software assurance specification standards,¹⁰ lay out a specific framework to document v&v activities.

The shuttle program recently tasked Intermetrics with documenting the processes NASA and its contractors follow in developing software, and highlighting the steps established to verify and validate the software.

⁷NASA Software Management Requirement for Flight Projects, NASA Management Instruction 2410.6, February 1, 1979.

⁸Software Assurance Guidebook, NASA-SMAP-GB-A201, September 1989.

⁹Management Plan Documentation Standard of the Information System Life-Cycle and Documentation Standards, Release 4.3, February 28, 1989.

¹⁰Assurance Specification Documentation Standard of the Information System Life-Cycle and Documentation Standards, Release 4.3, February 28, 1989.

However, such documentation had not been approved as of early December 1990.

Program Officials See Oversight as Sufficient

Although program officials are working to establish a v&v policy and improve documentation of v&v activities, they stated that they have no plans to implement the software v&v office advocated by the steering group because they believe the program already has sufficient v&v oversight. They cited examples of oversight provided specifically by the shuttle program office at Johnson, and generally by the headquarters-based program requirements control board. The Johnson-based shuttle avionics software control board also provides overall program direction to shuttle program components and contractors, and reviews and approves all changes to shuttle systems software prior to implementation. Program officials also cited the periodic performance reviews by NASA's Office of Safety and Mission Quality and the Office of the Inspector General. None of these, however, is specifically tasked with ensuring that (1) all v&v activities are effectively integrated into a coherent and coordinated process, (2) all contractor and NASA organizations and facilities perform required v&v activities, and (3) these activities' level of independence is adequate.

Further, officials mentioned that each major component manager in the process is required to sign certificates of flight readiness before each shuttle flight. By signing these certificates, signers certify that (1) the software has been developed in accordance with policies and procedures and will meet the needs of the mission, or that (2) they have identified and documented concerns about the software that they believe may affect the mission.

Shuttle V&V Approach Seen as Best Available

Shuttle program officials at Johnson stated they firmly believe that the independence built into the shuttle software v&v process is highly effective and is the best in the aerospace industry, pointing out that shuttle flights have never experienced significant software problems. They said that independence in the software v&v processes is achieved, without an independent contractor such as Intermetrics or a NASA office independent of the shuttle program office, by the requirement that separate contractor organizational elements, other than the software designers and developers, perform the v&v functions, and by the NASA program's inclusion of outside personnel in various oversight activities. Program officials point out—in the absence of their own program policy—that this approach is consistent with one followed by the Air Force, which

permits the v&v agent to be part of the prime contractor's organization, but must report to a level above the software development team.¹¹

The shuttle program's thinking on the level of independence required for software v&v may be consistent with Air Force policy, but it is not consistent with current NASA-wide software assurance guidance. NASA's software assurance guidebook,¹² which describes many types of v&v activities, defines independent v&v as

a process whereby the products of the software development life cycle phases are independently reviewed, verified, and validated by an organization that is neither the developer nor the acquirer of the software. The independent V&V agent should have no stake in the success or failure of the software. The independent V&V agent's only interest should be to make sure that the software is thoroughly tested against its complete set of requirements. [emphasis added]

The software development contractors who now develop, verify, and validate the software do not satisfy this definition of independence. Although both the primary and backup software contractors have established separate in-house groups for software development and for software v&v, they report to the same manager in their respective organizations. For example, the managers of IBM's Software Development Division and the Software Verification and Validation Division report to the same supervisor—the manager of on-board space systems. Further, all v&v activity is performed under the auspices of the NASA shuttle program office (the acquirer).

¹¹Software Independent Verification and Validation, AFSC/AFLC Pamphlet 800-5, Department of the Air Force, May 20, 1988, p. 19.

¹²Software Assurance Guidebook, NASA-SMAP-GB-A201, September 1989.

Conclusions and Recommendations

Although shuttle program officials believed that their v&v procedures were adequate when NRC and a congressional committee raised concerns in 1988, they promptly had one of their contractors, Intermetrics, begin independent v&v on shuttle software. They also established a knowledgeable steering group to examine the software v&v processes and suggest changes where appropriate. Despite these initial steps, NASA has made virtually no progress in improving v&v for shuttle software; its plans for v&v are a step backwards.

The steering group has yet to satisfy its charter. Although it raised several significant issues concerning v&v, it never recommended specific corrective actions. As a result, the program has yet to address its concerns—over 2 years after the group met in 1988. Program officials have begun developing a v&v policy and documenting v&v practices. These are certainly steps in the right direction, and will, if completed, bring NASA into closer alignment with industry standards, federal guidelines, and NASA's own software documentation standards.

Shuttle program officials contend they do not need an independent oversight office to ensure that all v&v activities are effectively integrated into a coherent and coordinated process, and that all contractor and NASA organizations and facilities perform required v&v activities. However, no single mechanism currently exists in the program to provide these assurances. Further, the program has maintained all along that its practice of having separate organizational elements perform v&v—within the same contractor but not the software designers or developers—effectively achieves an acceptable level of independence. We disagree.

We recognize, as did NRC, that NASA might have to rely on its network of contractors and facilities to perform basic v&v for most software. However, considering the billions of dollars already invested in the program and the significant risks involved, shuttle software is simply too critical not to have some level of independent v&v by an organization outside the control of the program office, possibly NASA's Office of Safety and Mission Quality. Although it never completed its work or developed formal recommendations, the software steering group was headed in this direction when it was dissolved.

The program officials' argument that independent v&v is not needed, on the basis of past flight successes and a belief that Intermetrics' v&v work did not discover any significant software errors in recent missions,

is not valid. Independent v&v is intended to provide a high level of additional assurance that the software will function as required. At its best, it should not discover any significant software errors. Given that NRC, NASA's own steering group, industry standards, federal guidelines, NASA's agencywide software assurance guidebook, and managerial prudence all support independent v&v for critical software such as that developed for the shuttle, the program's position that no independent v&v is needed is clearly a minority viewpoint and should not be accepted by the Administrator because the risks associated with this position are simply too great.

Recommendations

We recommend that the Administrator, NASA, require independent v&v for shuttle software, bearing in mind the views of NRC, the House Committee, the software steering group, and NASA-wide guidance, and that the Administrator ensure that the independent v&v organization is outside the control of the shuttle program office. In addition, we recommend that the Administrator bring to closure the issues raised by the software steering group concerning policy and documentation of v&v activities. In this regard he should require the steering group to provide formal recommendations and require the program office to provide time frames for addressing them.

Agency Comments

In commenting on a draft of this report, NASA concurred with our assessment of the critical issues associated with the development of shuttle software. NASA identified several positive actions it planned in response to the report. First, NASA said it would establish a steering committee to

- review the documentation and baselining of the existing independent v&v mechanisms,
- complete the drafting of the independent v&v policy statement for the shuttle program, and
- review the need for establishing a separate v&v office within the program and specify how that office would report on its work.

The agency plans to document and present the steering committee results and recommendations to headquarters for approval by June 30, 1991. Second, NASA said it would ask the steering committee, as part of a continuing oversight process, to review the shuttle program's v&v activities on an annual basis and report its findings and recommendations to high-level program officials. Finally, the agency said it plans to ask NRC

to perform a one-time independent review of the v&v process to evaluate its adequacy.

NASA's planned actions to bring the software steering group's issues to closure fully respond to our recommendations in this area. However, we question the need to restudy the shuttle software v&v process to evaluate its adequacy. These processes have been studied several times by different organizations, each reaching a similar conclusion—that while the shuttle software development activities are very good, more should be done. However, given the relatively short time frame established for the study, we are not opposed to NASA's obtaining another viewpoint. Our position is, however, unwavering: an appropriate level of independent v&v should be required. In addition, we believe that to be truly independent, the v&v office should be located outside the control of the shuttle program office.

Further, since several shuttle missions are scheduled to occur while NASA is conducting these planned activities, NASA should ensure that independent v&v is conducted. If the steering group recommendations or the NRC study result in a decision that independent v&v is not needed above the level NASA believes is already “embedded” in its processes, the Administrator should be prepared to explain and justify that decision to the House Committee on Science, Space, and Technology. NASA's comments are included as appendix I.

Comments From the National Aeronautics and Space Administration



National Aeronautics and
Space Administration

Washington, D.C.
20546

Office of the Administrator

JAN 23 1991

Mr. Ralph V. Carlone
Assistant Comptroller General
of the United States
General Accounting Office
Washington, DC 20548

Dear Mr. Carlone:

Thank you for your letter of December 19, 1990, enclosing the draft report "Space Shuttle: NASA Should Implement Independent Oversight of Software Development (GAO/IMTEC-91-20)." Your interest and concern in ensuring the safety and success of Space Shuttle missions through the monitoring of the critical flight software production process is appreciated.

We concur with your assessment of the critical issues associated with the development of flight software. In recent months, the Agency has embarked on a program to standardize and upgrade its software development and information systems to comply with the new Federal Security Regulations concerning Automated Information Systems (AIS). As part of this process, the NASA centers and program offices conducted several audits of both the methods and mechanisms employed in the software development, verification, validation, and certification processes. These audits afforded several opportunities to closely examine, from different perspectives, our embedded processes, including Independent Validation and Verification (IV&V) activities.

In a May 1988 letter from Dr. Fletcher, former NASA Administrator, to the House Committee on Science, Space, and Technology, we indicated that we would examine NASA's IV&V capability, in response to concerns raised by the House Committee. We set up a Steering Committee of senior personnel from government and Space Shuttle contractor organizations to review and recommend changes as appropriate to our IV&V process. We also engaged an experienced contractor, Intermetrics, Inc., to assist in this activity.

As a result of the Intermetrics assessment, we have incorporated all identified flight critical recommendations. We are in the process of reviewing the final IV&V process document. It will be used as the Space Shuttle program baseline of our embedded IV&V activities.

A review of your draft report has been conducted by cognizant individuals and program elements at both the field centers and Headquarters. Although we differ with the criticality associated with some of your findings, these differences do not have a strong bearing on our response. Where there is the potential for open work or discrepancy, the Space Shuttle program will determine the appropriate disposition for the identified items.

Considering the decade-long maturity of the Space Shuttle program, plus the review of our IV&V processes by an independent contractor, we conclude that there are sufficient, compelling reasons to continue to implement our contractor-embedded IV&V programs. We consider that the embedded contractor/government IV&V programs (e.g., Rockwell, IBM), which have recently undergone several audits, adequately address GAO's basic concerns associated with the critical flight software element of the Space Shuttle program.

Significant benefits have accrued to the program from our IV&V efforts to date. These include: (1) documentation of our embedded IV&V activities, which will be incorporated into a program baseline; (2) independent participation and involvement of NASA's Safety, Reliability, Maintainability, and Quality Assurance organizations in our processes; (3) implementation of recommended changes to the IV&V process via the efforts of Intermetrics, Inc.; and (4) maintenance of an independent contractor IV&V activity through the transition period to the new General Purpose Computers (GPC's). The first flight with the new GPC's, STS-39, is scheduled for February 1991.

In lieu of continuing the Intermetrics effort beyond the current fiscal year, the Space Shuttle program will ensure that the following actions are implemented. A Steering Committee will be tasked to review the documentation and baselining of the embedded IV&V mechanisms and to complete drafting the policy statement for the Space Shuttle IV&V Program. This committee may include some members of the original Steering Committee and other outside contractor and government personnel. This will ensure that objectivity is maintained.

The Steering Committee will also be tasked to review the need for establishing a separate IV&V office within the program and will specify the attendant reporting procedures. Committee recommendations and results will be formally documented and presented to Headquarters for approval with targeted completion by June 30, 1991.

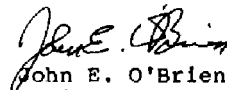
Appendix I
Comments From the National Aeronautics
and Space Administration

3

As part of the continuing oversight process, the Steering Committee will review the Space Shuttle IV&V Program on an annual basis. Findings and recommendations will be reported to the Associate Administrator for Space Flight and to the Director, Space Shuttle Program.

In addition, to ensure the validity of our approach, the National Research Council (NRC) will be asked to perform a one-time independent review of the process to evaluate its adequacy.

Sincerely,



John E. O'Brien
Assistant Deputy Administrator

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.

Ronald W. Beers, Assistant Director
Dr. Rona B. Stillman, Chief Scientist
Michael P. Fruitman, Supervisory Reports Analyst

Dallas Regional Office

Sherrill H. Johnson, Regional Management Representative
William H. Thompson, Evaluator-in-Charge
Sandra K. White, Staff Evaluator

Requests for copies of GAO reports should be sent to:

**U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877**

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are \$2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

